Surveillance de masse

Forget, Catherine

Published in:
Kairos

Publication date:
2016

Document Version
le PDF de l'éditeur

SURVEILLANCE DE MASSE : ENTRE SURVEILLANCE COMMERCIALE ET SURVEILLANCE RÉPRESSIVE

L'éventail de mesures de traitement de données à caractère personnel à grande échelle est multiple et ne cesse de se développer. Ainsi, récemment, le gouvernement se targuait d'adopter des nouvelles mesures visant à lutter contre le terrorisme dont le *Passenger Name Record* (PNR), qui suppose la création d'une base de données à partir des informations fournies par les sociétés de transport. Dans un autre registre, la rétention de données oblige les entreprises à collecter et stocker les métadonnées de l'ensemble des utilisateurs de réseaux de communications. Si l'arsenal s'étoffe, les autorités font fréquemment appel aux acteurs privés pour obtenir certaines informations. En effet, à l'heure du *big data*, la quantité de données traitées par des sociétés commerciales est exponentielle d'autant qu'elle constitue un enjeu financier notable. La surveillance de masse n'est donc pas qu'une simple affaire de «nouvelles mesures» censées apporter du grain à moudre aux enquêteurs, une surveillance basée sur la collaboration entre autorités publiques et acteurs privés est tout aussi intrusive.

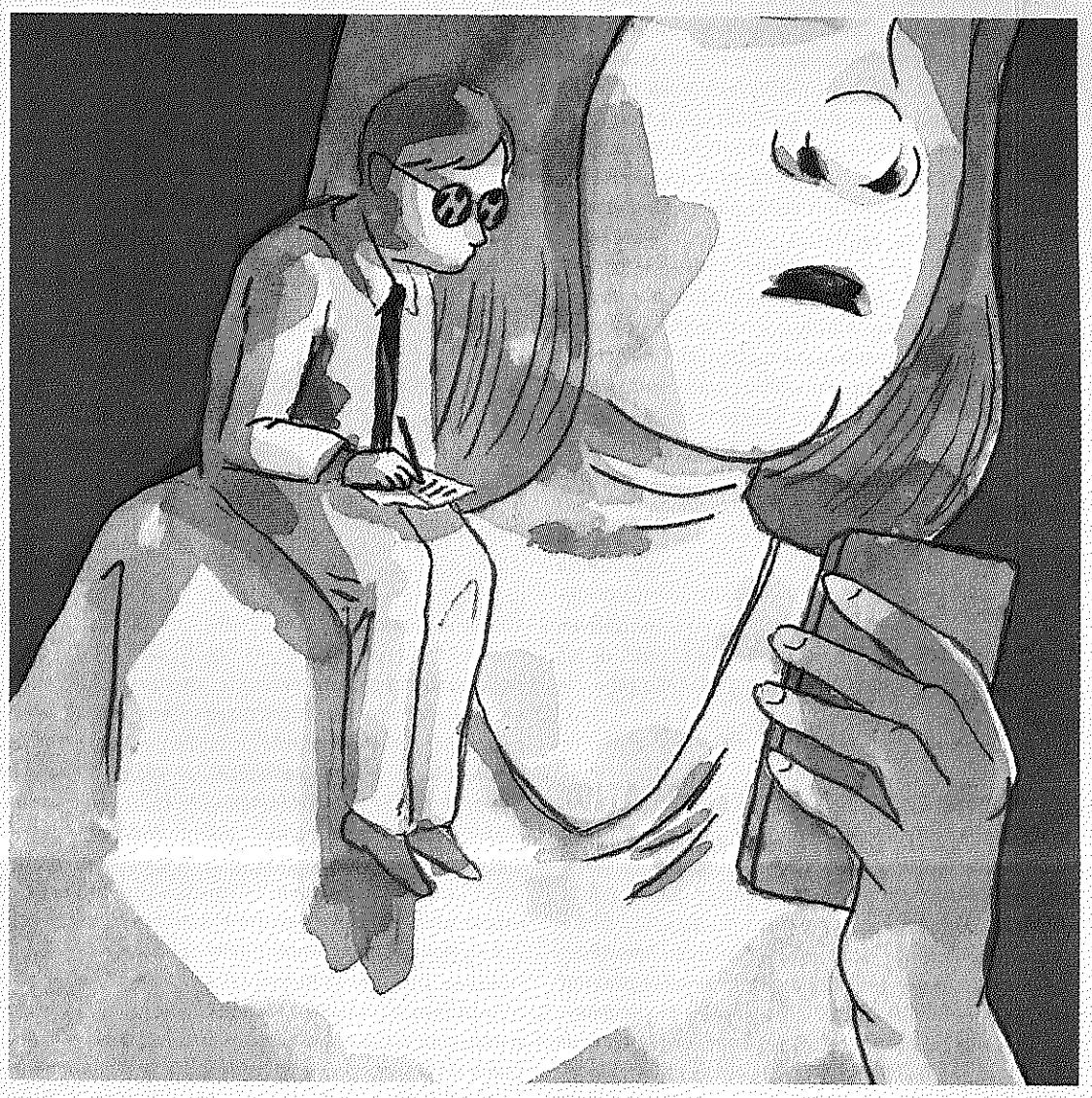

Illustration : Aurore Vegas

UNE AIGUILLE QUI NE CESSE DE SE PERDRE DANS LA BOTTE DE FOIN

La polémique relative au traitement de données à grande échelle occupe une partie de la scène médiatique depuis les révélations du lanceur d'alerte Edward Snowden, en juin 2013, lorsque ce dernier met en lumière les programmes de la National Security Agency (NSA) au moyen desquels les États-Unis interceptent au niveau mondial le contenu de nos communications. Ces données, collectées secrètement , sont susceptibles d'être transmises à des services de renseignements étrangers. En Belgique, par exemple, les services de renseignements peuvent utiliser des informations recueillies par la NSA sans être tenus de chercher à savoir si les données ont été collectées légalement[1].

Au niveau européen, le débat du traitement de données à grande échelle fut alimenté par l'implémentation d'une directive européenne relative à la rétention de données. Cette mesure impose aux opérateurs de télécommunications de collecter et de stocker l'ensemble des métadonnées: adresse IP, pseudonymes utilisés, listes de contacts, dates et heures d'envoi et de réception des courriers électroniques, sites internets consultés, dates et heures de connexion, etc. Les métadonnées, qui ne prennent pas en considération le contenu des communications ou des courriers électroniques, doivent être stockées durant une certaine période pour être accessibles (sur demande) aux autorités répressives. La rétention de données et le stockage de celles-ci s'opèrent donc *a priori*, de manière systématique et indifférenciée, indépendamment de l'ouverture d'une enquête pénale; l'accès aux données collectées par les autorités répressives suppose par contre l'existence d'une telle enquête.

La directive «*rétention de données*», une fois transposée en droit belge, fut directement portée devant la Cour constitutionnelle. Ses détracteurs invoquaient le caractère disproportionné d'une telle mesure vu la gravité de l'atteinte au droit à la vie privée. Ils soulignaient également le risque de stigmatisation de personnes présumées innocentes mais potentiellement suspectes, les données de l'ensemble des utilisateurs étant collectées sans aucun lien avec l'ouverture d'une enquête pénale. Le 8 avril 2014 - au niveau européen -, le 2 juin 2015 - au niveau belge -, la Cour de Justice de l'Union européenne et la Cour constitutionnelle ont invalidé et annulé les dispositions en cause. Les juges pointent l'absence de garanties suffisantes prévues par la mesure au regard de l'étendue des données collectées. La Cour constitutionnelle reprenant les termes de la Cour de Justice, relève en outre: «*La circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées* [...] *le sentiment que leur vie privée fait l'objet d'une surveillance constante*».[2] En effet, la rétention de données, même si elle ne concerne pas le contenu de nos communications, reste très intrusive dans la mesure où les métadonnées « *prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées* »[3]. Tant les juges européens que belges ont donc mis un (premier) frein au stockage massif et indifférencié des métadonnées. Leurs décisions imposent au législateur de revoir les dispositions afin de limiter l'atteinte à la vie privée au strict nécessaire, par exemple en prévoyant une durée de conservation de données plus courte. Premier frein étant donné qu'à l'heure où nous écrivons ces lignes, la Belgique est en passe d'adopter une nouvelle loi. Le sujet est donc loin d'être clos d'autant que la disposition adoptée dans la foulée des attentats de Londres et de Madrid en 2005 au niveau européen, n'a fait l'objet d'aucune étude suffisamment concrète permettant d'affirmer qu'elle est efficace à des fins de lutte contre la grande criminalité et le terrorisme.

Enfin, plus discrètement, le gouvernement s'apprête à se doter d'un *Passenger Name Record*, soit de prévoir un traitement de données des passagers. Le PNR à la belge vise à élaborer une base de données à partir des informations fournies par les usagers des compagnies aériennes, de trains et bateaux internationaux. Ce fichier national supervisé par le Service Public Fédéral Intérieur a la particularité d'être soumis à un algorithme particulier croisant certaines données afin d'établir des profils particuliers en vue de déceler les éventuels terroristes, mais aussi de lutter contre l'immigration illégale. A l'instar de la rétention de données, cette base de données est consolidée a priori, indépendamment de l'ouverture d'une enquête pénale, mais implique également un traitement de données à des fins de profilage. Cette mesure particulièrement critiquée pour son caractère «préventif», laisse également en suspens la question de l'efficacité du PNR pour at-

(1) A ce sujet, voir le rapport annuel du Comité R disponible à l'adresse suivante : http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2014.pdf

(2) C.J.U.E., 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12. 8 avril 2014. Point 37 et 65 C.C., 11 juin 2015, n°84/2015.

(3) Points 26-27 et 37 de l'arrêt Digital Rights.

teindre l'objectif poursuivi. A titre illustratif, les déplacements par véhicules motorisés comme ce fut le cas pour les attentats de Paris ne sont pas détectés, les bombes pourront toujours exploser aux entrées des aéroports comme ce fut le cas pour les attentats de Bruxelles, par exemple. De plus, en pleine lutte contre la fraude sociale voire en pleine lutte contre les assurés sociaux, face à cette manne d'informations, le risque de détournement de la finalité initiale est alléchante.

Les techniques de traitement de données à grande échelle mises en place par les autorités, sont donc surtout critiquées pour leur absence de proportionnalité considérant que «*la surveillance de masse a des répercussions potentiellement graves sur la liberté de la presse, la liberté de pensée et la liberté d'expression, ainsi que sur la liberté de réunion et d'association, et qu'elle entraîne un risque élevé d'utilisation abusive des informations collectées à l'encontre d'adversaires politiques*»[4]. Or, pour être conforme à la Convention européenne des Droits de l'Homme, une ingérence doit être nécessaire et proportionnée. Le législateur, avant l'adoption d'une disposition, est censé s'assurer qu'il n'existe pas d'autres mesures moins contraignantes ou permettant déjà d'atteindre le but poursuivi. En l'occurrence, outre l'absence de démonstration claire et avérée de l'efficacité d'un stockage massif et indifférencié de données à des fins de lutte contre le terrorisme, la nécessité de mettre en place de tels dispositifs peut également être mise en cause.

Illustration : Aurore Vegas

UN DÉPLACEMENT DE LA SURVEILLANCE VERS LES ACTEURS PRIVÉS

Les acteurs privés sont considérés comme des intervenants privilégiés dans le cadre d'enquêtes pénales dans la mesure, en traitant des données à des fins de marketing et de facturation, ils accèdent automatiquement à un ensemble de données à caractère personnel. Ces données une fois collectées, peuvent être stockées pendant une certaine période pour être soumises à des algorithmes particuliers. Sur Internet par exemple, nombres de services gratuits type Skype, Facebook, Google, Twitter, Youtube, Amazon... traitent nos données numériques «en masse» afin d'établir des profils de consommation. Le flux de données entre les acteurs privés et les autorités répressives est fréquent. En effet, en Belgique, les acteurs privés sont expressément tributaires d'une obligation de collaboration envers les autorités judiciaires; ils prêtent dès lors régulièrement leur concours dans le cadre d'enquêtes pénales. Un procureur peut solliciter auprès de fournisseurs d'accès à Internet semblables à VOO, Proximus, Telenet, certaines données de communications à savoir l'identité de l'abonné d'une ligne téléphonique, d'une adresse de courrier électronique, d'une connexion internet, d'une adresse IP, etc. Un juge d'instruction pourra croiser ces données pour, par exemple, géolocaliser une personne, identifier ses déplacements, intercepter ses communications ou intercepter ses courriers électroniques. Dans certains cas, ce dernier pourra également forcer les personnes présumées disposer d'une connaissance particulière d'un système informatique, à collaborer en bloquant l'accès aux données ou en fournissant la clé de chiffrement si les données sont cryptées. La personne sollicitée a la possibilité de se réfugier derrière le droit au silence, à condition d'être directement impliquée dans l'enquête. Enfin, certains intermédiaires et notamment les hébergeurs de sites internet, sont tenus de dénoncer au procureur du Roi les activités ou informations illicites dont ils auraient connaissance. Ils doivent également bloquer sur demande ou de leur propre initiative les sites «*incitant à la haine*» par exemple, ou faisant «*l'apologie du terrorisme*».

Si la plupart des sociétés se « prêtent au jeu », certaines refusent parfois de collaborer. Ainsi, Yahoo! a déjà contesté la demande d'un procureur lui imposant de communiquer certaines données. Le Parquet souhaitait déterminer l'identité de plusieurs utilisateurs d'adresses électroniques utilisées dans le cadre d'une affaire d'escroquerie. Néanmoins, Yahoo! ne voulait pas donner suite à la demande. La société motivait son refus en invoquant l'absence d'autorité de la loi belge à l'égard d'une entreprise américaine soumise au droit américain. De plus, elle contestait être tenue d'une obligation de collaboration puisque la demande émanait d'un procureur et non d'un juge d'instruction. En effet, le juge d'instruction peut faire intervenir l'ensemble des acteurs privés ou presque, alors que le Parquet devait se limiter, en principe, aux fournisseurs d'accès à Internet, c'est-à-dire par exemple VOO ou Proximus. La Cour de cassation a finalement tranché la controverse. Elle considère en premier lieu que la loi est applicable à toute entreprise «*qui fournit des mails en Belgique, participe à la vie économique (du pays)*». En second lieu, selon la Cour, l'obligation de fournir certaines données et de collaborer à la demande du procureur ne se limite pas aux fournisseurs d'accès à Internet tels que l'invoquait 'Yahoo!' mais s'étend à tout acteur offrant des services de communications électroniques. La nuance est importante puisque par cette interprétation, le juge permet au procureur d'obtenir des données auprès de la plupart des services disponibles sur Internet tels Skype ou Facebook, sans devoir faire appel au juge d'instruction. Or, l'ouverture d'une instruction est censée offrir à la personne inculpée l'apport de certaines garanties contre le risque d'accès illicites et arbitraires aux données.

Dans la même logique, récemment, la société Apple a refusé d'obtempérer à une injonction du FBI lui ordonnant de déchiffrer le téléphone portable d'un des auteurs de la tuerie de San Bernardino. Outre le déblocage du téléphone, le FBI souhaitait qu'Apple élabore une nouvelle version du système d'exploitation. Cette assistance technique aurait permis aux services répressifs américains de faciliter le déverrouillage de n'importe quel smartphone. Or, selon Apple, un tel logiciel facilitant l'accès aux téléphones met à mal la sécurité et la confidentialité des données stockées. En bout de course, le FBI finit par trouver une faille lui permettant d'accéder aux données contenues sur le téléphone. *In casu*, les services d'enquêtes américains vont plus loin que la «simple» obligation de collaboration exposée ci-avant. Les enquêteurs souhaitaient en effet forcer un acteur privé à concevoir des portes facilitant l'accès aux données contenues. En Belgique, une telle obligation n'existe pas mais pourrait se concevoir. Actuellement, la loi autorise par contre les services de renseignement à pirater un système informatique « *à l'aide ou non de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités* ». Ces derniers sont donc en mesure de s'immiscer dans un ordinateur en insérant un virus informatique par exemple et de collecter les informations souhaitées. Celles-ci pourront être transférées aux services de police si cela s'avère nécessaire.

En conséquence, si le traitement de données à grande échelle à travers des mesures telles l'obligation de rétention de données ou l'accord PNR fait couler beaucoup d'encre pour des raisons de proportionnalité, force est de constater que, outre l'absence d'efficacité démontrée *in concreto*, le caractère «nécessaire» de tels dispositifs pourrait également susciter un large débat. Les données des voyageurs collectées par les agences de voyage par exemple, sont déjà accessibles sur demande du procureur du Roi. De même, le Parquet a la possibilité d'accéder aux données de communications déjà conservées par les opérateurs à des fins commerciales indépendamment donc de l'existence d'une obligation de rétention. Sans parler du coût de telles mesures, le débat relatif à la surveillance de masse devrait donc être élargi. En effet, la frontière entre surveillance «de masse» commerciale et surveillance «de masse» sécuritaire est loin d'être étanche. Dès lors, un cryptage généralisé reste la réponse la plus efficace pour protéger notre vie privée.

Catherine Forget

(4) Ibid., point 10.